

CLAIMS

1. A method for preventing an administrator to  
 5 impersonate a user of a relational database, which  
 database at least comprises one table with at least one  
 user password, which password is used for logging on to  
 said database, wherein said password is stored as a hash  
 value, said method comprising the steps of:
- 10 adding a trigger to said table, said trigger at  
 least triggering an action when an administrator alters  
 said table through a database management system (DBMS)  
 for said database;
- calculating a new password hash value differing from  
 15 said stored password hash value when said trigger is  
 triggered; and
- replacing said stored password hash value with said  
 new password hash value.
2. A method according to claim 1, comprising the  
 20 further steps of:
- calculating a check value of said trigger, such as a  
 hash value; and
- comparing said trigger control value at the startup  
 25 and at regular intervals with a recalculated check value.
3. A method according to claim 1 ~~or 2~~, comprising  
 the further step of comparing for each active user having  
 access to sensitive data, the hash value of the current  
 30 login password with the hash value of the currently  
 stored password.
4. A method according to claim 3, wherein the  
 further step of comparing is performed after every change  
 35 of the database content by said user.

006277 5052/50

a

a

10

15

20

replacing means for replacing said stored hash value with said new hash value for each triggered calculation.